ALERT MEMORANDUM

Divided Supreme Court Requires Warrants for Cell Phone Location Data

July 2, 2018

On June 22, 2018, the United States Supreme Court decided *Carpenter v. United States*, in which it held that the government must generally obtain a search warrant supported by probable cause before acquiring more than seven days of historical cell-site location information ("CSLI") from a service provider.[1]

The Court grounded its decision upon the "seismic shifts in digital technology" brought about by the ubiquitous use of cellphones that the Court recognized in its 2014 decision in *Riley v. California*, and the discomfort expressed by several justices in the Court's 2012 decision in *United States v. Jones* with long-term surreptitious location monitoring.[2] Noting "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection," [3] the Court held in *Carpenter* that an individual "maintains a legitimate expectation of privacy in the record of his physical movements captured through CSLI" that warrants Fourth Amendment protection.[4]

In doing so, the Court took the notable step of imposing an express limitation on the third-party doctrine that has historically limited privacy expectations with respect to information provided by individuals to third parties (in this case, the cell phone carriers that collected CSLI). While the Court sought to construe its decision narrowly, the reasoning of the majority and that of Justice Gorsuch in his dissent raise significant questions about whether and to what extent individuals may have a reasonable expectation of privacy or possessory interest in other sensitive personal data held by third parties beyond the CSLI at issue in *Carpenter*.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

NEW YORK

Jonathan Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

WASHINGTON

Alexis Collins
+1 202 974 1519
alcollins@cgsh.com

Laura Gavin
+1 202 974 1623
lgavin@cgsh.com

Anne Hilby
+1 202 974 1635
ahilby@cgsh.com

Tanner Mathison
+1 202 974 1548
tmathison@cgsh.com

[1] 585 U.S. __ (2018).
[2] *See id.* at 15; *Riley v. California*, 573 U.S. __, 134 S. Ct. 2473 (2014) (holding that cell phones cannot generally be searched incident to arrest absent a warrant in part because of the vast scope of private information they contain); *United States v. Jones*, 565 U.S. 400, 415, 430-431 (2012) (concurring opinions by J. Alito and J. Sotomayor that "longer term GPS monitoring . . . impinges on expectations of privacy").
[3] Slip Op. at 22.
[4] *Id.* at 11.

Background

Carpenter involved the prosecution of multiple defendants for a series of armed robberies of electronics stores.[5] During its investigation, the government obtained court orders to collect telephone records—including CSLI—associated with several cell phones used by various suspects including the petitioner, Timothy Carpenter.[6] As the Court described, CSLI is a "time-stamped record" of each time a cell phone or similar device connects with an antenna that is attached to a cell tower (or "cell site") in the wireless network, which generally occurs multiple times every minute. The record of the date and time of the connection combined with the location of the cell site and direction of the antenna to which the cell phone connects provides information that may be used to determine an articulable radius where the phone was located at a particular time.[7] Pursuant to the orders, the carriers provided 129 days of cell-site location information.[8]

The orders were granted by a magistrate judge pursuant to a provision of the Stored Communications Act, 18 U.S.C. § 2703(d), which compels disclosure of certain categories of records upon provision of "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records . . . are relevant and material to an ongoing criminal investigation."[9] This standard is less demanding than that traditionally required for a search warrant, which is probable cause to believe that the records contain evidence of a crime.

The District Court Decision

Carpenter was ultimately charged with multiple criminal violations in connection with the robberies.[10] Prior to trial, Carpenter moved to suppress his cell phone records—which included his cell-site location information—on the basis that they had been collected in violation of the Fourth Amendment.[11] Carpenter argued that cell phone users have a reasonable expectation of privacy in "prolonged surveillance data," and thus a probable cause standard—not a "reasonable grounds" standard—was required under the Fourth Amendment to obtain the cell-site data.[12] The district court denied Carpenter's motion, relying on established precedent that rejected the notion of a cognizable expectation of privacy in cell-site data because it is "'simply a proxy' for the defendant's visually observable location, and a defendant has no legitimate expectation of privacy in his movements along public highways."[13]

At trial, the government used the cell-site data to show that Carpenter's cell phone was in the vicinity of the relevant stores at the time of the robberies. Based on this and other evidence, Carpenter was convicted on numerous charges.[14]

The Sixth Circuit Decision

On appeal, the Sixth Circuit again rejected Carpenter's argument that collection of CSLI was a search under the Fourth Amendment for which probable cause is required.[15] In affirming the court below, the appellate court principally relied on two long-established lines of Fourth Amendment jurisprudence. It distinguished cell-site data from the content of personal communications, in which courts have recognized a reasonable expectation of privacy. Instead the court likened it to routing information used to "facilitate personal communications" (such as the address on an envelope, phone numbers dialed, and email headers) for which the Supreme Court had repeatedly declined to find a reasonable expectation of privacy. Moreover, the Sixth Circuit found Carpenter

[5] *See United States v. Carpenter*, No. 12-20218, 2013 WL 6385838, at *1 (E.D. Mich. Dec. 6, 2013).
[6] *See id.*
[7] *See* Slip Op at 1-2.
[8] *See id.* at 3.
[9] *Id.* at 3.
[10] *See United States v. Carpenter*, 819 F.3d 880, 884-85 (6th Cir. 2016).
[11] *See Carpenter*, 2013 WL 6385838, at *1.
[12] *Id.* at *1-2.
[13] *Id.* at *2 (quoting and citing *United States v. Skinner*, 690 F.3d 772, 777, 779 (6th Cir. 2012)).
[14] *See Carpenter*, 819 F.3d at 885.
[15] *Id.* at 890.

had no cognizable property interest in the cell-site data because it was collected and maintained by third parties—the cell phone carriers—in the ordinary course of business. Thus, the court reasoned that the carriers' collection and disclosure to the government of CSLI was not a search of the defendant's property that is protected by the Fourth Amendment.[16]

On this basis, the appellate court distinguished the government's collection of CSLI from a third-party telephone carrier from its attachment of a GPS tracker to an individual's car, which five Supreme Court justices had agreed in *Jones* raised Fourth Amendment privacy concerns.[17] It reasoned that, not only was the "nature of the state activity" at issue in *Jones* strikingly different (*i.e.*, collecting "business records . . . from a third party" versus "secretly attach[ing] a GPS device" to a vehicle), but cell phone location data is not nearly as accurate as GPS data, which could potentially reveal intimate details of an individual's daily life.[18]

The Supreme Court Decision

In a 5-4 decision authored by Chief Justice Roberts, and joined by Justices Ginsburg, Breyer, Sotomayor, and Kagan, the Court held "that the Government must generally obtain a warrant supported by probable cause before acquiring [CSLI]."[19] All four dissenting justices wrote separate dissenting opinions.

Chief Justice Roberts' Majority Opinion

The Court grounded its decision in the same two lines of Fourth Amendment case law considered by the Sixth Circuit, although the Court came to the opposite conclusion. The Court turned first to cases involving the expectation of privacy in physical location and movement. Likening the privacy concerns raised by CSLI with those raised by GPS tracking in *Jones*, the Court held that individuals maintain an "expectation of privacy in the record of [their] physical movements."[20] The Court noted that, despite generally providing less precise location data than GPS information, CSLI presents "even greater privacy concerns" than GPS tracking as cell phones have become "a feature of human anatomy" that have enabled "near perfect surveillance" into a person's life.[21] The Court further stressed that the "retrospective quality of CSLI . . . gives police access to a category of information otherwise unknowable" and permits retroactive surveillance of everyone, "not just . . . persons who might happen to come under investigation."[22] These privacy interests thus gave rise to a reasonable expectation of privacy in CSLI.

The Court then examined whether that expectation of privacy in CSLI was lost under the so-called "third-party doctrine" in *Smith*, which provides that individuals have "no legitimate expectation of privacy in information [they] voluntarily turn[] over to third parties,"[23] such as financial records shared with a bank[24] or dialed telephone numbers conveyed to a telephone company.[25] The Court declined to extend the third-party doctrine to CSLI maintained by third-party cell phone carriers based on the strong privacy interest in locational data and the involuntary nature of its collection.[26] In the Court's view, unlike bank records and telephone numbers, CSLI can provide a "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[27] Moreover, cell phone users do not voluntarily "share" CSLI with carriers in the normal sense of the word, as cell phones typically log location information without "any affirmative act on the part of the user beyond powering up."[28]

[16] *See id.* at 886-88 (citing *Smith v. Maryland*, 442 U.S. 735 (1979); *Katz v. United States*, 389 U.S. 347 (1967)).
[17] *See id.* at 888-89 (citing *Jones*, 565 U.S. 400).
[18] *See id*. (quoting *Smith*, 442 U.S. at 741).
[19] Slip Op. at 18.
[20] *Id.* at 11.
[21] *Id.* at 13 (citing *Riley*, 573 U.S. at __, 134 S. Ct. at 2484).
[22] *Id*.
[23] *Id.* at 9 (quoting *Smith*, 442 U.S. at 743-44).
[24] *See United States v. Miller*, 425 U.S. 435, 440-443 (1976).
[25] *See Smith*, 442 U.S. 735 at 742-45.
[26] *See* Slip Op. at 11-12.
[27] *Id.* at 17.
[28] *Id.*

In light of the above, the Court concluded that the acquisition of CSLI associated with Carpenter's device for periods of seven days or more constituted a search under the Fourth Amendment that generally required a warrant supported by probable cause.[29] Since the "reasonable grounds" standard of Section 2703(d) of the Stored Communications Act, through which the government had obtained Carpenter's CSLI, fell "well short of . . . probable cause," it could not be used to obtain historical cell-site records.[30] As a result, the Court reversed the Sixth Circuit and remanded the case for further proceedings consistent with its opinion.

Despite its broad pronouncements about the privacy interest in location information, the Court framed its decision as a narrow one affecting only the "rare case where the suspect has a legitimate privacy interest in records held by a third party."[31] The Court clarified that the traditional warrant exceptions (such as exigent circumstances) still apply to CSLI in appropriate situations and that the government can use subpoenas to compel production of records in which a suspect lacks a legitimate privacy interest.[32] The Court also expressly declined to reach the questions of whether a request for CSLI spanning fewer than seven days could be permissible without a warrant[33] or how other types of business records that reveal location information or "other collection techniques involving foreign affairs or national security" might fare under the third-party doctrine moving forward.[34]

The Dissents

Despite the majority's attempt to limit its holding, the decision drew separate opinions from all four dissenting justices. Justices Kennedy, Thomas, Alito, and Gorsuch each advocated for a return to a property-based approach to the Fourth Amendment. Justice Kennedy found that the case was governed entirely by the third-party doctrine of *Smith* and *Miller*, and that CSLI was "no different" from other kinds of business records the government may obtain from third parties simply by subpoena, without a showing of probable cause.[35] Justice Alito similarly concluded that that an order "requiring a party to look through its own records and produce specified documents" is not a search, and that defendants have no Fourth Amendment right "to object to the search of a third party's property."[36] Justice Thomas likewise urged the Court to focus on Carpenter's lack of a property interest in CSLI, but further called upon the Court to abandon the reasonable expectation of privacy test set forth in *Katz* in its entirety.[37]

Somewhat surprisingly, Justice Gorsuch also advocated a return to a property-based approach to the Fourth Amendment,[38] but one that could potentially justify the same result reached by the majority—application of a warrant requirement to CSLI. As an example of that approach, he proposed treating certain third-party control of data as "a sort of involuntary bailment" in which the individual retains a cognizable protected legal interest in the data. Using this approach, Justice Gorsuch recognized the possibility that "a person's cell-site data could qualify as his papers or effects under existing law," but criticized Carpenter for failing to fully develop the argument below.[39]

Impact and Implications

The most direct impact of the Court's decision in *Carpenter*, of course, is to significantly limit the government's ability to use Section 2703(d) orders to obtain CSLI information. Though the Court expressly limited its decision to orders seeking at least seven days of CSLI held by cell phone carriers, its effects could have far-reaching implications for companies as well as law enforcement.

[29] *See id.* at 17-18.
[30] *Id.* at 18-19.
[31] *Id.* at 21.
[32] *Id.* at 21-22.
[33] *See id.* at 11 n.3.
[34] *Id.* at 18.
[35] *See* Opinion of Kennedy, J., dissenting, at 1-2 (citing *Miller*, 425 U.S. 435; *Smith*, 442 U.S. 735).
[36] Opinion of Alito, J., dissenting, at 1-2.
[37] Opinion of Thomas, J., dissenting, at 1-2, 17-21.
[38] *See* Opinion of Gorsuch, J., dissenting, at 6-9.
[39] *Id.* at 20-21.

First and foremost, *Carpenter* raises significant questions about whether and to what extent the Court's treatment of CSLI will extend Fourth Amendment protection to other categories of personal information held by third parties. The majority took pains to distinguish the privacy concerns driven by the "unique nature of cell phone location information"[40] from those of data it characterized as less robust, such as financial records[41] and telephone toll records.[42] But like cell phones that collect CSLI, other technologies, such as wearable devices, connected vehicle technology, and smart appliances, among others, are increasingly capable of tracking individuals' movements and associations "every day, every moment, over several years."[43] And like cell phones, the use of such technology will only become more pervasive over time. The opinion leaves open the possibility for courts to find that individuals have a similar privacy interest in data collected through other devices.

Moreover, as Justice Kennedy noted, the logic of the majority and Justice Gorsuch calls into question whether traditional business records, such as credit card records, could in the future be found to trigger a legitimate expectation of privacy. As the economy trends away from the use of cash in favor of electronic transactions, government collection of bank records could arguably yield an equally "detailed chronicle" of an individual's movements and activities over large spans of time.[44] Given the broad language in the majority opinion, lower courts will likely be forced to wrestle with this issue in the coming years. Open questions likewise remain as to whether third parties may, or could be pressured by customers to, challenge administrative or grand jury subpoenas for other types of personal data on Fourth Amendment privacy grounds.

Carpenter also plunged the Supreme Court into the growing debate about whether and to what extent individuals have a possessory interest in personal data collected and stored by a third party. Both the majority and Justice Gorsuch engaged on the question of whether CSLI should receive the protections typically granted to an individual's papers and effects.[45] Their discussion echoed questions that have been increasingly raised in Congress about who owns personal data collected by businesses, most recently during last year's hearings on the Equifax Data Breach.[46] These questions raise significant considerations for any business that collects personal consumer data since, as Justice Thomas' and Justice Gorsuch's dissents noted, property, contract, or tort law may recognize possessory interests in personal data and thus could enable recovery from third-parties for the loss or misuse of personal data.[47]

For these reasons, questions about the reach of *Carpenter* and the existence of possessory interests in personal data collected by private businesses could give rise to a flood of Fourth Amendment challenges and provide further impetus to state and federal legislation efforts in this area.[48] They could also create

[40] Slip Op. at 11.
[41] *See Miller*, 425 U.S. 435.
[42] *See Smith*, 442 U.S. 735.
[43] Slip Op. at 16-17.
[44] *Id*.
[45] *See id.* at 21 (arguing that "a detailed log of a person's movements over several years" should receive the protections afforded to the "modern-day equivalents of an individual's own 'papers' or effects'"); Opinion of Gorsuch, J., dissenting, at 20-21 (recognizing that "a person's cell-site data could qualify as his papers or effects under existing law").
[46] For example, in an October 2017 hearing, Representative Matsui asked "if data that you hold is about me do I own it? Do I own my data?" *See Oversight of the Equifax Data Breach: Answers for Consumers Before the Subcomm. on Digital Commerce and Consumer Protection of the H. Comm. on Energy and Commerce*, 115th Cong. 74 (2017).
[47] *See* Opinion of Thomas, J., dissenting, at 36-37 (noting that current law does not convey a property right in CSLI); Opinion of Gorsuch, J., dissenting, at 17 (noting ongoing legislative efforts to define users' rights over data and digital accounts).
[48] Indeed, as noted below, less than a week after *Carpenter* was released, California adopted sweeping new privacy legislation that provides individuals with more control over information collected about them by private companies, including the right to know what information is being collected as well as the sources of such information and how it is being used, and the right to demand that such data be

a "blizzard of litigation" by private litigants asserting a possessory interest in data held by businesses of all types.[49]

Given the potential wide-ranging impact of the Supreme Court's decision, particularly when combined with ongoing political and constituency support to legislate increased individual privacy protections (such as with a law recently passed in California), organizations that collect and hold personal data should continue to monitor the evolving standards of data privacy law, including what constitutes a reasonable expectation of privacy in the age of modern technology.

…

CLEARY GOTTLIEB

deleted. For additional background on the scope and requirements of this legislation, see Rahul Mukhi, Daniel J. Esannason & Zekariah McNeal, California Introduces Bill Expanding Consumer Rights Over Data Privacy, *Cleary Cybersecurity and Privacy Watch Blog* (June 27, 2018), https://www.clearycyberwatch.com/2018/06/california-introduces-bill-expanding-consumer-rights-data-privacy/.

[49] *See* Opinion of Alito, J., dissenting, at 1.